Amendments to the drawings,

There are no amendments to the Drawings.

Remarks

Status of application

Claims 1-64 are pending in the application. Claims 1-64 stand rejected on the basis of prior art. Claims 49 and 50 have been amended to correct informalities. Claims 9, 20, and 38 have been amended to provide antecedent basis where required. In view of these amendments and the clarifying remarks made below, re-examination and reconsideration of the claims are respectfully requested.

The invention

Applicant's invention comprises a system providing methods for a security component on a router (or other client premises equipment) to check compliance of a computing device with an access policy before permitting the computer to access the Internet. Applicant's system delegates a portion of the overall operation of a security solution to a local piece of client premises equipment (e.g., router) which enforces compliance with an access policy. Every few seconds a router-side security component of the present invention sends a communication referred to as a "router challenge" to computers on the local network. The router challenge requests the local computers to respond with information indicating whether or not they are in compliance with the access policy. At the local computers, a client-side security component of the present invention prepares and returns a response to the router challenge. The responses provided by the local computers (if any) are then evaluated by the router-side security component to determine whether each local computer is in compliance with the access policy. The result of this compliance check is stored at the router.

Each time the router receives a request to connect to the Internet from a particular local computer, the router-side security component determines whether or not the particular computer properly responded to the most recent router challenge. If the computer properly responded to the challenge and was determined to be in compliance with the access policy, then the router permits the computer to access the Internet. However, if the computer did not answer the router challenge or responded with information indicating that it was not in compliance with the policy, then it is not allowed to connect to the Internet. Instead, the non-compliant computer is redirected to a "sandbox" server to address the non-compliance. Generally, the non-compliant computer is only permitted to connect to the sandbox server for performing a defined set of tasks and all other Internet access by the non-compliant computer is disabled.

Oath/Declaration

The Examiner has indicated that the oath or declaration filed by Applicant is defective as it does not identify the mailing address of each inventor and does not identify the city and either state or foreign country of residence of each inventor. Enclosed herewith is a newly-signed Declaration (PTO Form PTO/SB/01), which lists the mailing address and citizenship of each inventor.

Claim Objections

The Examiner has objected to claims 49 and 50 as containing informalities requiring correction. Claims 49 and 50 have been amended to correct these informalities.

Claim Rejections under 35 USC Section 112

The Examiner has rejected claims 9, 20, and 38 under 35 USC Section 112, second paragraph as indefinite, for lack of antecedent basis. The claims have been amended to provide antecedent basis where required, thus overcoming the rejection under Section 112, second paragraph.

Prior Art Rejections

A. Double Patenting

The Examiner has rejected claims 8, 9, 10, 11, 12, 17, 18, 20, 32, 33, 34, 35, 38, 53, 54, 55 and 57 under the doctrine of obviousness-type double patenting as being unpatentable over claims 1, 6, 7, 11, 12, 19, and 21 of U.S. Patent No. 5,987,611 ("the '611 patent"). The Examiner cites In re Longi, 759 F.2d at 896, 225 USPQ at 651 (Fed. Cir., 1985) and In re Berg 140 F.3d at 1437, 46 USPQ2d at 1223 (Fed. Cir., 1998) that a later patent claim is not patently distinct from an earlier patent claim if the later claim is obvious over, or anticipated by, the earlier claim. The Examiner states that claims 1, 6, 7, 11, 12, 19, and 21 of the '611 patent "contain every element of claims 9, 18, 11, 33, 55, 12, 8 &10, 32, 53, 20, 38, 54, 34, 35, 17 and 57 of the instant application" and as such anticipate these claims (Examiner office action, paragraph 6). The rejection is traversed for the reasons stated below.

As will be demonstrated, the Examiner's rejection under the doctrine of obviousness-type double patenting is inappropriate as claims 8-12, 17, 18, 20, 32-35, 38, 53-55 and 57 of the present application are patently distinct from claims 1, 6, 7, 11, 12, 19, and 21 of the '611 patent. Claims 8-12, 17, 18, 20, 32-35, 38, 53-55 and 57 of the present application are patently distinct from the referenced claims of the '611 patent as they include claim limitations that are not found in the earlier claims. A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in the single prior art reference. (See, e.g., MPEP Section 2131.) As demonstrated below, these claims of the present application include elements not found in the earlier '611 patent and, therefore, are patentably distinct from, and not anticipated by, the claims of the '611 patent.

At the outset, it should be noted that each of claims 8-12, 17, 18, 20, 32-35, 38, 53-55 and 57 that the Examiner states are anticipated by the '611 patent are dependent claims which incorporate the limitations of other claims that the Examiner has not indicated as being anticipated by the '611 patent. For instance, claims 8-12, 17, 18, and 20 of the present application are dependent upon, and incorporate the limitations of, independent claim 1 (as well as any intervening claims). Similarly, claims 32-35 and 38 are dependent upon, and incorporate the limitations of independent claim 24, and claims 53-55 and 57 incorporate the limitations of independent claim 45. As such, the claims rejected by the Examiner include several claim limitations which are not found in the referenced claims of the earlier '611 patent, thereby demonstrating that these claims are patently distinct from those of the '611 patent.

For example, the Examiner indicates that claim 9 of the present application corresponds to, and is anticipated by, claim 1 of the '611 patent. However, comparing these claims shows that claim 9 of the present application incorporates claim limitations not found in claim 1 of the '611 patent. For instance, claim 1 of the '611 patent makes no mention of client premises equipment (e.g., a router) serving a routing function for client computers, nor does it indicate that the client premises equipment issues challenges to client devices for determining whether the clients are in compliance with an access policy before permitting the clients to access the Internet. Rather, claim 1 of the '611 patent describes a security system which operates locally at a client computer as follows:

> 1. In a system comprising a plurality of client computers connected to a network and having Internet access, a method for managing Internet access for a particular client computer, the method comprising:
> providing at the particular client computer a client monitoring process;
> providing at another computer on the network a supervisor process, said supervisor process specifying rules which govern Internet access by the client computers;
> transmitting at least a subset of said rules to the particular client computer;
> at the client monitoring process, trapping a request for Internet access from the particular client computer; and
> processing the request for Internet access by performing substeps of:
> (i) determining whether the request for Internet access violates any of the rules transmitted to the particular client computer, and
> (ii) if the request for Internet access violates any of the rules transmitted to the particular client computer, denying the request for Internet access.
>
> (Claim 1, U.S. Patent No. 5,987,611, emphasis added)

Significantly, claim 1 of the '611 patent makes no mention of client premises equipment serving a routing function for client computers. As illustrated above, it provides that compliance with rules governing Internet access is evaluated by a client monitoring process at the client computer. In addition, claim 1 of the '611 patent does not include claim limitations of transmitting a challenge to the client computers (whether from client premises equipment or otherwise), nor does it include the element of blocking a request for Internet access by any client computer that does not respond to the challenge. The present invention provides for a piece of client premises equipment (e.g., a router) to serve in a compliance enforcement role by challenging client machines accessing the Internet to ensure they are in compliance with rules of an access policy. Claim 9 of the present application, as amended, references and incorporates the limitations of claim 8. Claim 8, in turn, incorporates the limitations of Applicant's claim 1, as follows:

> 1. In a system comprising one or more client computers connected to the Internet by client premises equipment serving a routing function for client computers, a method for managing Internet access based on a specified access policy, the method comprising:
> transmitting a challenge from said client premises equipment to each client computer, for determining whether a given client computer is in compliance with said specified access policy;
> transmitting a response from at least one client computer back to said client premises equipment, for responding to said challenge that has been issued; and blocking Internet access for any client computer that does not respond appropriately to said challenge.
>
> (Applicant's claim 1, emphasis added)

Claim 1 of the '611 patent provides for a client-side component to receive a set of rules and apply these rules at a given client for determining whether or not to permit Internet access at the client. This does not, however, address the problem of an environment (e.g., a local LAN) served by a router (or other client premises equipment) that includes one or more client machines that have not installed the client-side component. Consider, for example, the case of a client device that has not installed the client-side component required by the access policy and which connects to the router to obtain Internet access. Absent any enforcement mechanism at the router, this client device is able to access the Internet even though it is not compliance with the access policy. The present invention provides for the router to serve a security enforcement role to verify that all machines obtaining Internet access through the router have installed client-side security software and are otherwise in compliance with a specified access policy (Applicant's specification, page 19, lines 19-29).

Claim 9 and the other claims of the '611 patent referenced by the Examiner do not include any teaching of a router or other client premises equipment that monitors connected client devices and enforces compliance with an access policy as provided in Applicant's specification and claims. As the '611 patent does not include all elements of claims 8-12, 17, 18, 20, 32-35, 38, 53-55 and 57 of the present invention, it does not anticipate these claims. Accordingly, Applicant respectfully submits that claims 8-12, 17, 18, 20, 32-35, 38, 53-55 and 57 are patently distinct from those of the '611 patent, thus overcoming the double patenting rejection.

B. Claim Rejections under 35 USC Section 102

Claims 1, 3-6, 8, 11, 12, 17, 21, 45, 46, 47, 48-51, 55 and 57 stand rejected under 35 U.S.C. 102(e) as being anticipated U.S. Patent No. 6,463,474 B1 issued to Fuh et al (hereinafter "Fuh"). The Examiner's rejection of Applicant's claim 1 as follows is representative of the Examiner's rejection of Applicant's claims:

> With respect to claim 1, Fuh et al discloses: In a system comprising one or more client computers connected to the Internet by client premises equipment serving a routing function for client computers (figure 3 item #306, item #210, item #216), a method for managing Internet access based on a specified access policy (see abstract), the method comprising: transmitting a challenge from said client premises equipment to each client computer (figure 4 item #403), for determining whether a given client computer is in compliance with said specified access policy; transmitting a response from at least one client computer back to said client premises equipment, for responding to said challenge that has been issued (figure 4 item #404); and blocking Internet access for any client computer that does not respond appropriately to said challenge (figure 7A block #707).
>
> (Examiner office action, paragraph 8)

Under Section 102, a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in the single prior art reference. (See, e.g., MPEP Section 2131.) As will be shown below, Fuh fails to teach each and every element set forth in independent claims 1 and 45 (as well as other claims), and therefore fails to establish anticipation of the claimed invention under Section 102.

Fuh describes an authentication proxy on a firewall router for authenticating users attempting to access resources (e.g., an Intranet) protected by the firewall router. Fuh's system is focused on authenticating users seeking access to resources based on login information supplied by these users. Fuh's authentication proxy requests user login information (e.g., user name and password) from users and verifies this user login information (Fuh, col. 7, line 48 to col. 8, line 6). Fuh also describes authentication cache (s) for storing user login information about users that have been authenticated (Fuh, col.

9, lines 56-59). When a packet (e.g., HTTP packet) directed to an Intranet or other resource is received, the firewall router of Fuh attempts to authenticate client identifying information in the packet (e.g., source IP address in the header field of the HTTP packet) that is received at the firewall router against entries a standard access control list (Fuh, col. 10, lines 25-34). If the source IP address of the request is found in a standard access control list, an authentication cache is searched for a matching entry as follows:

> If the test of block 706 is affirmative, then control passes to block 708 in which the authentication caches are searched for the source IP address. In block 710, the process tests whether the source IP address is found. For example, if Authentication Proxy 400 determines that the source IP address matches at least one IP address stored in the filtering mechanism 219, then the Authentication Proxy 400 attempts to authenticate the user 302. In the preferred embodiment, Authentication Proxy 400 searches authentication caches 432, 434 for the source IP address. The goal of this search is to determine if the source IP address of the HTTP packet corresponds to an entry in any of the authentication caches 432, 434.
>
> (Fuh, col. 10, lines 35-47, emphasis added)

As described above, Fuh's system is focused on authenticating a user based on login information (e.g., username and password), rather than on examining the state of computing device that the user is utilizing. It should also be noted that Fuh's system does not proactively issue challenges to client devices. Instead, it waits to receive a request for access to particular resources (e.g., Intranet) and then attempts user authentication. Fuh's system also includes authentication caches for storing information about users that have previously been authenticated. Before issuing a request to the user to provide user login information (e.g., username and password) for authentication purposes, Fuh's system consults these authentication cache(s) for determining if the user has previously been authenticated. If no matching entry is found in the authentication cache, a new entry is created in the cache and Fuh's authentication proxy attempts to authenticate the client by requesting a username and password as follows:

> **Referring again to FIG. 7B, after the new authentication cache is created, login information is requested from the client, as shown in block 724.** For example, Authentication Proxy 400 obtains authentication information from User

> 302 by sending a login form to client 306. **The login form is an electronic document that requests User 302 to enter username and password information, as shown by path 403.**
>
> (Fuh, col. 11, lines 49-55, emphasis added)

As described above, Fuh's authentication proxy requests a user to enter a username and password in a login form for authenticating the user. Fuh's system determines whether or not to permit access to the resources to a particular user based on this user login information. If the login information supplied by the user is correct and the authentication process is successful, access is permitted and the authentication cache is updated so that subsequent requests can authenticate locally at the firewall router (Fuh, col. 12, lines 38-47).

In contrast to Fuh's system which is focused on authentication of a user based on standard user login information, Applicant's system focuses on the state of the client computer. Applicant's router-side security component issues challenges to client computers for determining compliance of the client computers with an access policy governing Internet access. Applicant's system does not permit or block requests based solely on user login information. Instead, **Applicant's system checks whether client computers are in compliance with rules of an access policy before permitting Internet access**. The access policy governing Internet access focuses on the state of the client computers and may, for instance, require particular security software to be installed on the client computers. If the required security software is not installed on a given computer, Applicant's invention regulates (e.g., blocks) access to the Internet until the computer is brought into compliance with the access policy (e.g., by installation of the required security software).

The periodic "router challenges" issued to client computers for evaluating compliance with the access policy may, for example, request information to verify that a particular version of a software program is installed on the client computer(s) on the local LAN (Applicant's specification, page 33, line 11 to page 34, line 9). As another example, with an "anti-virus challenge" option specified in the access policy, the router-side security module issues a challenge requesting information about anti-virus software running on the client computer in order to evaluate whether the anti-virus program and the associated data file (virus definition file) meet the requirements specified in the access policy. The challenge issued by the router may also request each of the local clients to respond indicating whether an "auto update" option of the required anti-virus software is activated (Applicant's specification, page 34, line 23 to page 35, line 10). If a given client computer does not respond appropriately indicating that the required software is installed and in operation as required by the policy, the router-side component of Applicant's system blocks access to the Internet by the given computer (Applicant's specification, page 21, lines 21-26). The router-side security component verifies that client computers are running required software and are in compliance with other policy requirements as follows:

> This router-side security component, running on the router or other piece of local client premises equipment, checks to ensure that appropriate end point security software is in place on all of the computers on the LAN. Prior to allowing a local computer to connect to the Internet, the security component on the router verifies that the computer has installed and is running appropriate security software, and is in compliance with other established security policies.
>
> (Applicant's specification, page 19, lines 22-27, emphasis added)

As illustrated above, Applicant's invention focuses on the state of the client computer and not on the identity of its user. Another difference between Applicant's system and that of Fuh is that Applicant's router-side security component proactively issues challenges to one or more client computers (e.g., computers on local LAN served by router) to verify compliance with the access policy. Fuh's system, in contrast, reacts to particular requests for access to resources (e.g., access to Intranet) received at a firewall router. Applicant's router-side component broadcasts a router challenge packet to one or more clients on the LAN every N seconds, as determined by a monitoring frequency setting established by an administrator (Applicant's specification, page 33, lines 3-7). This enables compliance to be evaluated on an ongoing basis, and not just on initial login. The clients are requested to respond with information responsive to the challenge (e.g., indicating whether or not the particular software required by the policy is installed and is running). These limitations of issuing a challenge to a client computer for determining compliance with an access policy are specified in Applicant's claims including, for example, claim 1, which provides as follows:

> 1. In a system comprising one or more client computers connected to the Internet by client premises equipment serving a routing function for client computers, a method for managing Internet access based on a specified access policy, the method comprising:
> **transmitting a challenge** from said client premises equipment to each client computer, **for determining whether a given client computer is in compliance with said specified access policy**;
>
> (Applicant's claim 1, emphasis added)

When a challenge is received by a client, a response packet is prepared and returned in response to the router challenge (assuming a client-side component of the present invention is installed at the client). The response includes information (e.g., the version of the particular software running at the client) which is responsive to the router challenge (Applicant's specification, page 35, lines 4-10). Based on the responses received from each of the clients (if any), the router-side component at the client premises equipment determines whether they are in compliance with the access policy (Applicant's specification, page 22, line 22 to page 23, line 4). Grounds for blocking Internet access by a client computer may include, for example, failure to receive a response to the router challenge, failure to run a current anti-virus program, or use of an outdated version of the security software. These limitations of clients responding to the challenge and the router-side component blocking access to clients that do not respond appropriately to the challenge indicating compliance with the access policy are also specified in Applicant's claims including, for example, claim 1:

> transmitting a response from at least one client computer back to said client premises equipment for responding to said challenge that has been issued; and **blocking Internet access for any client computer that does not respond appropriately to said challenge**.
>
> (Applicant's claim 1, emphasis added)

This is also specified, for instance, in Applicant's claim 45 which includes the following limitations:

> an access policy governing Internet access by said client computers;
> client premises equipment serving a routing function for each client computer to be regulated and capable of issuing a challenge to each client computer, for determining whether a given client computer is in compliance with said access policy;
> one or more client computers which can connect to the Internet and at least one of which can respond to challenges issued by said client premises equipment; and
> an enforcement module for selectively blocking Internet access to the Internet to client computers not in compliance with said access policy.

(Applicant's claim 45, emphasis added).

Applicant's router-side security component proactively issues challenges to client computers to check whether the client computers are in compliance with rules of an access policy. This router-side component then selectively blocks Internet access by client computers which either do not respond to the challenges or which respond indicating that they are not in compliance with the access policy. In this manner, Applicant's system regulates access to the Internet based on compliance by the client computer with requirements of the access policy. Fuh, in contrast, is focused on authentication of a user based on standard user login information and provides no comparable teaching of checking client computers for compliance with an access policy governing Internet access. As Fuh does not teach or suggest all of the claim limitations of Applicant's independent claims 1 and 45 (and other claims) it is respectfully submitted that the claims distinguish over this reference and overcome any rejection under Section 102.

C. First Rejection under 35 USC Section 103(a)

The Examiner has rejected claims 2, 7, 10, 13-16, 18-19, 20, 47, 52-54, 56, 58-60 under 35 U.S.C. 103(a) as being obvious over Fuh. The Examiner acknowledges that Fuh does not explicitly disclose elements of these claims, but states that the elements not explicitly disclosed in Fuh would have been obvious to one ordinarily skilled in the art. The Examiner's rejection of Applicant's claims 13-16 as follows is representative of the

Examiner's rejection of Applicant's claims as obvious over Fuh:

> As per claims 13-16, Fuh et al does not explicitly disclose: application are specified by executable name and version number, application are specified by digital signatures, digital signatures are computed using a cryptographic hash and wherein said cryptographic hash comprises a selected one of Secure Hash Algorithm (SHA-l) and MDS cryptographic hashes, however it would have been obvious to the one of ordinary skill in the art to use the above specified elements because it would have allowed a router to make a correct decision (block or permit) by comparing executable names and securely transfer the data to the destination.
>
> (Examiner office action, paragraph 14)

Under Section 103(a), a patent may not be obtained if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which the subject matter pertains. To establish a prima facie case of obviousness under this section, the Examiner must establish: (1) that there is some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings, (2) that there is a reasonable expectation of success, and (3) that the prior art reference (or references when combined) must teach or suggest all the claim limitations. (See e.g., MPEP 2142). As will be shown below, the references cited by the Examiner fail to meet the requisite condition of teaching or suggesting all of Applicant's claim limitations.

Claims 2, 7, 10, 13-16, 18-19, 20, 47, 52-54, 56, 58-60 are dependent upon independent claims and therefore are believed to be allowable for at least the reasons cited above pertaining to the deficiencies of Fuh in respect to Applicant's invention. As described above, Fuh does not teach a router-side component that periodically issues challenges to client computers for evaluating compliance of such client computers with rules of an access policy. Additional differences between Applicant's invention and that of Fuh are illustrated in Applicant's dependent claims. For example, Applicant's claim 13 includes as claim limitations that applications approved for Internet access are "specified by executable name and version number that are acceptable." This is also described in Applicant's specification, including, for example, the following:

> Many other policies may also be enforced in addition to those that are shown. For example, an administrator may permit a local computer to access the Internet using Internet Explorer, but deny access to the Internet if the application on the local computer initiating the connection is a RealAudio player because of the significant bandwidth that is used by the RealAudio application.
>
> (Applicant's specification, page 27, lines 22-25)

Applicant's careful review of the Fuh reference finds no comparable teachings of permitting particular applications installed on a client computer to access the Internet and blocking access by other applications in the manner described in Applicant's specification and claims. The Examiner references Fuh at column 7, lines 56-58 for the teaching of an access policy specifying applications that are allowed Internet access. However, the referenced portion of Fuh reads as follows:

> If the username is successfully authenticated, then the firewall is dynamically configured to open a passageway for the HTTP packets as well as other types of network traffic initiated from the user on the client. The other types of network traffic that are permitted through the passageway are specified in a user profile for that particular user.
>
> (Fuh, col. 7, lines 56-58, emphasis added)

As described above, Fuh's system receives identity information (e.g., username and password) for authenticating a user. Once the user identity is authenticated, Fuh's system permits particular types of network traffic by that user. However, Fuh provides no teaching or suggestion of examining whether particular applications or versions are installed on a computer, nor does Fuh teach or suggest identifying the application on the computer that is requesting Internet access for determining whether Internet access by that application is to be permitted or blocked in the manner specified in Applicant's specification and claims. Accordingly, as the Fuh reference does not teach or suggest all of the claim limitations of Applicant's claims, it is respectfully submitted that the claims distinguish over these references and overcome any rejection under Section 103.

D. Second Rejection under 35 USC Section 103(a)

The Examiner has rejected claims 22-25, 27-37, 39, 40, and 42 under 35 U.S.C. 103(a) as being obvious over Fuh in view of U.S. Patent No. 5,761,683 to Logan et al. (hereinafter "Logan"). The Examiner acknowledges that Fuh does not explicitly disclose the elements of redirecting a client computer that is not in compliance with the access policy to a sandbox server and adds Logan for these teachings.

These claims, which incorporate the limitations of Applicant's independent claims, are believed to be allowable for at least the reasons cited above pertaining to the deficiencies of Fuh in respect to Applicant's invention. Logan does not cure the above-described deficiencies of Fuh as it provides no teaching of a router-side security component which monitors and enforces compliance by client computers with rules of an access policy. Furthermore, Applicant's review of Logan finds that it does not include the specific teaching set forth in Applicant's claims of redirecting a client determined not to be in compliance with the access policy to a "sandbox" server for remedying the non-compliance as provided in Applicant's claim 24:

> transmitting a challenge from said client premises equipment to each client computer, for determining whether a given client computer is in compliance with said specified access policy;
> transmitting a response from at least one client computer back to said client premises equipment, for responding to said challenge that has been issued; and
> redirecting a request for Internet access by any client computer that does not respond appropriately to said challenge to a sandbox server.
>
> (Applicant's claim 24, emphasis added)

The referenced portions of Logan cited by the Examiner simply discuss conventional steps of handling requests for remotely stored documents by redirecting certain requests to retrieve locally stored copies and sending other requests to the remote web server(s) which return either the information (e.g., HTML document, graphical image, FTP file, or other displayable data) or an error message if the attempt to obtain the information does not succeed. This does not teach anything analogous to Applicant's claimed approach of redirecting a client determined not to be in compliance with the access policy to a particular "sandbox server" for purposes of remedying the non-compliance. As the combined references do not teach or suggest all of the claim limitations of Applicant's claims, it is respectfully submitted that the claims distinguish over these references and overcome any rejection under Section 103.

E. Third Rejection under 35 USC Section 103(a)

The Examiner has rejected claims 26 and 41 under 35 U.S.C. 103(a) as being obvious over Fuh in view of Logan, further in view of U.S. Patent No. 6,026,440 to Shrader et al (hereinafter "Shrader"). The Examiner acknowledges that Fuh and Logan do not explicitly disclose the element of permitting a client computer to elect to access the Internet after displaying error messages, but adds Shrader (col. 4, lines 56-57) for the teaching of "returning an error message (e.g., Unauthorized) to the browser and prompting the user for id and password" (Examiner office action, paragraph 24).

Claims 26 and 41, which incorporate the limitations of Applicant's independent claims, are believed to be allowable for at least the reasons cited above pertaining to the deficiencies of Fuh and Logan in respect to Applicant's invention. Shrader does not cure the above-described deficiencies of Fuh and Logan. The referenced portion of Shrader simply provides that a check is made for credentials of a user and, if the user does not have appropriate credentials, Shrader's system returns an error message and requests username and password from the user. This does not teach Applicant's claim limitations of a router-side security module which evaluates and enforces compliance by client computers with rules of an access policy, nor does it provide the specific teaching of Applicant's claims 26 and 41 of permitting a client computer not in compliance with the access policy to elect to proceed with Internet access notwithstanding the failure to comply with the access policy. As the combined references do not teach or suggest all of the limitations of Applicant's claims, it is respectfully submitted that these claims distinguish over these references and overcome any rejection under Section 103.

F. Fourth Rejection under 35 USC Section 103(a)

The Examiner has rejected claim 61 under 35 U.S.C. 103(a) as being obvious over Fuh in view of US Patent No. 6,542,933 to Durst, Jr. et al (hereinafter "Durst"). Claim

61, is believed to be allowable for at least the reasons cited above pertaining to the deficiencies of Fuh in respect to Applicant's invention. Durst does not cure these deficiencies. The referenced portions of Durst simply discuss receiving a URL request at an information server and redirecting the request to a content server to receive a content file. Durst provides no teaching of issuing challenges for evaluating compliance of a client computer with an access policy or for redirecting client computers determined not to be in compliance with the access policy to a sandbox server as provided in Applicant's claims. As the combined references do not teach or suggest all of the limitations of Applicant's claims, it is respectfully submitted that these claims distinguish over these references and overcome any rejection under Section 103.

G. Fifth Rejection under 35 USC Section 103(a)

The Examiner has rejected claims 62-64 under 35 U.S.C. 103(a) as being obvious over Fuh in view of Durst, further in view of Shrader. These claims, which incorporate the limitations of Applicant's independent claims, are believed to be allowable for at least the reasons cited above pertaining to the deficiencies of Fuh, Durst and Shrader in respect to Applicant's invention. As the combined references do not teach or suggest all of the limitations of Applicant's claims, it is respectfully submitted that these claims distinguish over these references and overcome any rejection under Section 103.

Conclusion

In view of the foregoing remarks and the amendment to the claims, it is believed that all claims are now in condition for allowance. Hence, it is respectfully requested that the application be passed to issue at an early date.

If for any reason the Examiner feels that a telephone conference would in any way expedite prosecution of the subject application, the Examiner is invited to telephone the undersigned at 408 884 1507.

Respectfully submitted,

Date: March 2, 2005

Digitally signed by John A. Smart
Date: 2005.03.02 14:05:12 -08'00'

John A. Smart; Reg. No. 34,929
Attorney of Record

408 884 1507
815 572 8299 FAX